

REMARKS/ARGUMENTS

This paper is being provided in response to the March 2, 2006 Final Office Action for the above-referenced application. In this response, Applicant has amended Claims 1, 22, 36, 47, and 54 in order to clarify that which Applicant deems to be the claimed invention. Applicant respectfully submits that the amendments to the claims and all newly added claims are supported by the originally filed application.

Applicant thanks the Examiner for the indication of allowance of Claims 26-30, 39-46, and 55-60.

Applicant also thanks the Examiner for the indication of allowability of Claim 54 if rewritten in independent form to include all limitations of the base claim and any intervening claims.

In response to the objection to Claim 54, Applicant has rewritten Claim 54, in accordance with remarks set forth in the Office Action, to be in independent form including all limitations of the base claim and any intervening claim. In view of the forgoing, Applicant respectfully requests reconsideration of the objection and submits that Claim 54 is now in condition for allowance.

The rejection of Claims 1-7, 13-16, 18-20, 22, 36, 47, 49, 50 52 and 53 under 35 U.S.C. § 103(a) as being unpatentable over Wells (U.S. Patent No. 6,338,141, hereinafter referred to as “Wells”) in view of Frisch Essential System Administration (hereinafter referred to as “Frisch”), Kim “The Design and Implementation of Tripwire: A File System Integrity Checker”

(hereinafter “Kim”), and Ko (U.S. Patent No. 6,697,950, hereinafter “Ko”). Applicant respectfully submits that the claims, as amended herein, are patentable over the cited art, taken separately or in combination.

Claim 1, as amended herein, recites a method of detecting computer viruses, comprising: providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments; an antivirus unit, that uses a particular operating system, scanning at least part of the disk space for viruses, wherein the part of the disk space that is scanned by the antivirus unit includes at least some parts of the first and second segments; the antivirus unit accessing non-native files created using operating systems different from the particular operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses, wherein said antivirus unit scans at least one of the segments without using file-based information of the particular operating system or of any host having access to said at least one segment; detecting write operations to tracks of the storage device; and performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed. Claims 2-7, 13-16, 18-20, and 52-53 depend from Claim 1.

Claim 22, as amended herein, recites a method of scanning a storage device for viruses, comprising: performing a first virus scan at a first time; and performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and

second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, scanning of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part, and wherein at least one of said performing said first virus scan and said performing said second virus scan includes: detecting write operations to tracks of the storage device; and performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

Claim 36, as amended herein, recites a computer program product for scanning a storage device for viruses, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, scanning of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part, wherein at least one of said means for performing said first virus scan and said means for performing said second virus scan include: means for detecting write operations to tracks of the storage device; and means for performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed.

Claim 47, as amended herein, recites an antivirus unit, comprising: means for performing a first virus scan at a first time; and means for performing a second virus scan at a second time after the first time, wherein for said second virus scan, logical entities having a date of last modification that is after the first time are examined and wherein performing said first and second virus scans includes using a particular operating system and accessing non-native files created using operating systems different from the particular operating system, wherein, when performing a virus scan accessing at least one part of the storage device that is also accessible to at least one host, scanning of said at least one part is performed without using file-based information of the particular operating system or of any host having access to said at least one part; wherein at least one of said means for performing said first virus scan and said means for performing said second virus scan includes: means for detecting write operations to tracks of the storage device; and means for performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed. Claims 49-50 depend from Claim 47.

Wells relates to a stand-alone computer process that uses a single information engine to produce a collection of relational data to detect computer viruses in computer files. The entire process is performed on a single, stand-alone computer system in real time. The process can also be run on the stand-alone system from a connected, remote computer system, which remote system can maintain the known virus databases. (See Abstract; Col. 1, Lines 5-20). Wells discloses a system called Raven as part of a virus detection tool. Raven is run on a given system and the gathered data for each file checked is tested against the relational data that represents the

known viruses stored in a virus-detection database. An exact match of all related data indicates a known virus is present. In addition, if most, but not all, of the data is matched, there is a high probability that an unknown (but closely related) virus is present. (Col. 2, Lines 54-62; Figure 5). Page 3 of the Office Action states that Wells does not expressly disclose providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments.

As set forth on page 3 of the Office Action, Frisch teaches a UNIX operating system that enables a flexible partitioning capability wherein each partitioned segment is accessed using a different file system. The Office Action also states on page 3 that Frisch discloses exporting local filesystems by a particular system for network access by other hosts to mount their system.

Page 4 of the Office Action cites Kim as teaching to selectively check the integrity of separate file systems on a disk using the UNIX tool tripwire.

The reference of Ko is cited on page 5 of the Office Action as support for disclosing techniques of scanning for viruses without using file-based information of the particular operating system or of any host having access to the at least one segment (Col. 1, Line 65-Col. 2, Line 3).

Applicant's Claim 1, as amended herein, is neither disclosed nor suggested by the references taken separately or in combination, in that the references neither disclose nor suggest at least the features of *a method of detecting computer viruses, comprising: ... the antivirus*

unit accessing non-native files created using operating systems different from the particular operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses, wherein said antivirus unit scans at least one of the segments without using file-based information of the particular operating system or of any host having access to said at least one segment; detecting write operations to tracks of the storage device; and performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed, as set forth in amended Claim 1.

Applicant respectfully submits that the teachings of Wells, Frisch and Kim suggest using file-based information of the particular operating system used by the antivirus unit in connection with scanning for viruses, rather than *without using file-based information of the particular operating system or of any host having access to said at least one segment* and rather than *detecting write operations to tracks of the storage device; and performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed,* as set forth in amended Claim 1. Ko discloses, at Col. 1, Line 65-Col. 2, Line 1, performing pattern matching on code to determine whether a known virus is present but appears silent regarding more specifically how the code in connection with pattern matching is accessed. Ko appears to neither disclose nor suggest *detecting write operations to tracks of the storage device; and performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed,* as set forth in amended Claim 1.

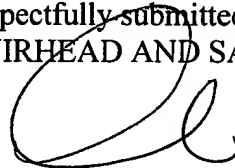
For at least these reasons, Applicant respectfully submits that Applicant's amended Claim 1 is patentable over the references.

Independent Claims 22, 36, and 47 recite features similar to those as pointed out above which are neither disclosed nor suggested by the references. Thus, Applicant respectfully submits that Claims 22, 36 and 47 are also not disclosed or suggested by the references.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

Based on the above, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections and objections. Favorable consideration and allowance are earnestly solicited. Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at 508-898-8604.

Respectfully submitted,
MUIRHEAD AND SATURNELLI, LLC



Anne E. Saturnelli
Registration No. 41,290

MUIRHEAD AND SATURNELLI, LLC
200 Friberg Parkway, Suite 1001
Westborough, MA 01581
Tel: (508) 898-8604
Fax: (508) 898-8602

Date: June 1, 2006